International Atomic Energy Agency, Vienna | Post No. **05/ISI-002**

JOB DESCRIPTION FOR PROFESSIONAL POSTS

The following job description should be completed in duplicate and forwarded through your Departmental Administrative Officer to the Division of Personnel when (1) a classification review of an existing post is proposed, (2) a new post is established requiring classification and recruitment action, or (3) the duties of a post have changed significantly. Where there is an incumbent in the post, the description should be completed jointly by the incumbent and immediate supervisor. If the post is vacant, the immediate supervisor should complete the description. Considerable care should be given in completing the job description as it will serve as the primary source of information in evaluating the grade level of the post and in preparing the vacancy notice.

Part I. GENERAL DATA

1. This job description is being submitted for the purpose of:

a) Requesting a review of the classification
b) Issuing a vacancy announcement
c) Redescribing the duties of an existing post
X d) Other (please explain): **Cost-free expert**

2. Location of post:

a)	Department	**Department of Safeguards**
b)	Division	**Division of Safeguards Information Technology**
c)	Section	**Section for System Infrastructure Support**
d)	Unit	**Systems and Communications Unit**

3. Functional title and current grade of post: **IT Vulnerability Expert (P4)**

CCOG code: **1A05C : Computer Specialists**

4. Present incumbent's name: N/a

Former incumbent's name:

If new post, please indicate date of establishment:

5. Incumbent's supervisor

a)	Name	Richard Gronvius
b)	Functional title	Unit Head
c)	Grade	P5

6. Date post was last reviewed: **N/a**

7. List the major changes in the duties of the post which have taken place since the last review. Note that existing posts will not be reviewed for reclassification purposes unless the duties and responsibilities have changed substantially since the current grading of the post was established and appear to be of a lasting nature. For reclassification procedures please refer to AM II/3, paragraphs 31-34.

N/a

---

8. Please show under this item the organizational structure of the Division. This can be done easily by inserting in the blank boxes the appropriate information. The "organizational" chart should show specifically (a) where the post is located in the hierarchy of the Department, (b) who reports to the post holder, (c) to whom the post holder reports.

Department level:	Department of Safeguards
Division level:	Division of Safeguards Information Technology
Section level:	Section for System Infrastructure Support
Unit level:	Systems and Communications Unit

---

9. If applicable, please list characteristic quantitative data relevant to the post. For example, in the case of an Editor, the number of pages edited may be of relevance for determining time spent on a task.

The Systems and Communications Unit currently supports approximately 1,500 devices and 700 people, ensuring reliable and secure networking, email, file repository, and application services, both in headquarters and at three established remote locations, as well as for staff on field duty throughout the world.

The Unit supports several virtual LANs with varying levels of security, from unclassified to highly confidential. The average number of IT protocol checks and firewalls between a user and associated data is six.

---

10. What are the main purposes (objectives) of the post? (Overall role/functions of the post with stress being placed on the more important aspects.)

1. To configure tools for continuous and regular intrusion detection and reporting.

2. To establish information and communication technology (ICT) standards, policies and procedures for the efficient and secure operation of the network and associated services.

3. To establish daily operating procedures to ensure that any decrease in reliability and any attempt to penetrate the network are detected and remediated.

4. To evaluate the ICT logical and physical architectures to identify and eliminate any potential reliability or confidentiality vulnerabilities.

5. To provide technical support and advice in the area of vulnerability for proposals for new network-based services.

Part II. JOB DESCRIPTION

Guidelines for Preparation:

This form is intended to obtain information about the job and not about the individual who may occupy the job, although it may be difficult to separate the job from the incumbent. Supervisors should ensure that the form describes the characteristics of the job that needs to be done and not the characteristics of the person doing the job. It is suggested that the description of each major duty begin with an action verb.

READ THROUGH THE ENTIRE FORM BEFORE STARTING TO COMPLETE IT

---

1. **Summarize the major duties and responsibilities of the position in order of importance and indicate in the margin the percentage of time spent on each (most jobs contain no more than 5 or 6 major responsibilities). First state what is being done, then how it is being done.**

% of time:	Duty/responsibility:
40%	Configuring Vulnerability Detection Tools Be familiar with vulnerability detection and intrusion detection tools, especially the IBM Tivoli and Symantec suite of tools. Configure these tools for continuous inspection of the safeguards networks, with regular reporting of incidents to appropriate staff.
30%	IT Vulnerability Operations Establish standards, guidelines, and processes for handling vulnerability incidents, including establishing realistic and useful daily reliability and security checking routines (i.e. "morning check", "services dashboard", and similar)
20%	Vulnerability Assessments Assess – through penetration testing, including technical and social measures – the vulnerabilities of the safeguards networks
10%	Technical Advice Participate in evaluations of logical and physical network models, evaluations of options for network components, and reviews of change proposals for network configurations.

---

2. **What are the minimum knowledge requirements of the job? (These need not be equivalent to those of the present incumbent.)**

Level and field of study of university degree (or the equivalent acquired through training or self-study)	University degree in Computer Science, or similar, with emphasis on networking and security.
Minimum length and type of practical	7 years of working experience in the area of

experience required:

ICT vulnerability management. Thorough knowledge of and experience with Tivoli tools, Symantec, CISCO and Netscreen products, telecommunications protocols, security technologies and protocols. Thorough knowledge of Microsoft network and server architectures, including specifically Active Directory. Knowledge of authentication tools and content inspection tools is an advantage.

- at national level
- at international level

Language(s): **English**

- proficiency required
- other languages preferred

---

3. Work Role: What does the job require the incumbent to do (i.e. describe the analysis, interpretation, adaptation, innovation, planning, co-ordination, and directing that the job requires)?

Plan and organize the implementation of configurations for tools to manage intrusion detection on a continual basis.

Design and recommend policies, guidelines, and procedures to monitor vulnerability incidents and to respond to these incidents.

Develop plans for and execute penetration tests of the safeguards networks.

Advise and report on technical issues related to vulnerability management.

---

4. What subject matter (diversity of work) does the job cover and what is the depth of treatment of the subject matter?

The incumbent is expected to apply his/her specialist technical and application knowledge of ICT vulnerability management in his/her assignment. This includes:

- Effective application of computer technology in a large international ICT environment, with several security levels and protection environments;
- A detailed knowledge of data communication technologies, security technologies, and the interaction between complex hardware and software systems, server configurations, local and wide area networks;
- A detailed knowledge of intrusion detection technologies, including configuration of tools (especially Tivoli and Symantec) and processing of reports from these tools;
- A good knowledge of performance and reliability monitoring technologies and their installation and configuration.

Knowledge of and experience with ITIL quality assurance processes, especially change management and incident management, is very useful.

---

5. Describe the control exercised or guidance given by the supervisor in terms of planning, controlling and reviewing the incumbent's work, e.g. how often do you meet, how are priorities handled, how is work achieved, how are instructions given.

The incumbent is expected to work within project definitions and supervision from the Head of Unit. He/She will be guided by the standards established by the Agency and the Department of Safeguards in the areas of information security, IT security, and ICT architecture. This is an independent level with a high degree of accountability for self controlled work. All products developed by the incumbent will be tested before being put into production.

6. Indicate which regulations, manuals, precedents, policies, or other administrative and technical guidelines apply to the incumbent's work, and to what extent the incumbent is permitted to interpret, deviate from, or establish new guidelines:

The incumbent is expected to comply with IAEA rules and regulations, Safeguards Agreements, which legally define the responsibilities of the Safeguards Department, and the Safeguards Manual, which prescribes regulations, policies and guidelines in achieving these responsibilities. The incumbent needs to be familiar with various technical manuals relating to Microsoft Server, Active Directory, network protocols and other products which interact with them.

The incumbent is expected to recommend changes to policies related to ICT vulnerability management as needed, to contribute relevant chapters in the Safeguards Manual, and to prepare technical guidelines. He/She will be required to use judgement and interpretation in applying these standards.

7. With whom (indicate title only), for what purpose, and how often is the incumbent required to have contacts in the job? (Describe the most typical, not the most unusual, contacts, e.g. to obtain information, to seek funding, to commit the Agency on .....)

	Person(s) title	Purpose	How often?
Inside the IAEA	Peers	To discuss technical issues	Daily
	Regional Offices	To discuss specific ICT vulnerability issues to these locations	Regularly
	Division Staff	To discuss specific ICT vulnerability issues arising from remote monitoring and field communications activities	Weekly
Outside the IAEA	N/A – much of the work of the incumbent will be classified.		

8. Describe the most important type(s) of decisions the incumbent is authorized to take and why these are important:

One of the most important decisions the incumbent is authorized to take is the design and configuration of intrusion detection and vulnerability management systems. This affects the security, integrity, availability and performance of the Department-wide services.

Another important decision taken by the incumbent is the design of the daily procedures and incident handling procedures. This affects the reliability and performance of safeguards networks.

---

9. **Describe the <u>most important</u> types of proposals expected of the incumbent in the job and why these are important:**

The incumbent will recommend to the supervisor changes to policies and standards on IT security, which affect the security, integrity, availability and performance of safeguards networks. He/She will propose innovative methods for minimizing risks to network reliability and security.

---

10. **Describe the <u>most damaging</u> involuntary error(s) that could be made in the work and the <u>effect(s)</u> that would result:**

An incorrect installation or configuration of vulnerability management tools could lead to weaknesses in the system not being discovered, making it vulnerable to security breaches.

---

11. **Total staff in organizational units supervised by incumbent. (Note: "supervised" means "held accountable for the work.") This is the only factor that is not applicable to all posts.**

Professional and higher level staff		Technical and administrative support staff	
<u>Grade level</u>	<u>number</u>	<u>Grade level</u>	<u>number</u>
n/a		**n/a**	

This is an accurate and complete description of the details of the job.

Incumbent	Date	Immediate Supervisor	28-2-2006 Date
Printed name:		Printed Name: **J. Barton**	
2-3-2006 Division Director	Date	060308 Administrative Officer	Date
Printed name: **J. Baute**		Printed Name: **A. Baute-Wiles**	

(Personnel - JD/P Apr. 1998)